

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)	
)	
Pasi Matti Kalevi AHONEN)	Group Art Unit: Unassigned
)	
Application No.: Unassigned)	Examiner: Unassigned
)	
Filed: January 18, 2001)	
)	
For: Virtual Private Networks)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination, please amend this application as follows.

IN THE SPECIFICATION

Page 1, line 3, delete "Field of the Invention" and insert therefor --Background--;

line 9, delete "Background of The Invention"; and

line 22, delete "Whilst" and insert therefor --While--.

Page 2, line 1, delete "Summary of the Invention" and insert therefor --Summary--;

and

line 26, delete "ISAKMP" and insert therefor --Internet Security Association
Key Management Protocol (ISAKMP)--.

Page 3, line 2, delete "authorise" and insert therefor --authorize--.

Page 5, line 12, delete "Detailed Description of a Preferred Embodiment" and insert
therefor -- Detailed Description--;

line 15, after "documents" insert --, the contents of which are incorporated by reference herein--;

line 24, delete "organisation's" and insert therefor --organization's--;

line 26, delete "organisation's" and insert therefor --organization's--; and

line 32, delete "utilises" and insert therefor --utilizes--.

Page 6, line 28, delete "Whilst" and insert therefor --While--;

line 30, delete "Firstly" and insert therefor --First--; and

line 32, delete "Secondly" and insert therefor --Second--.

Page 11, line 24, delete "whilst" and insert therefor --while--; and

line 27, delete "optimisations" and insert therefor --optimizations--.

Page 13, line 23, delete "Initialisation" and insert therefor --Initialization--.

Page 16, line 19, delete "utilising" and insert therefor --utilizing--.

Page 18, line 4, delete "practise" and insert therefor --practice--;

line 23, delete "whilst" and insert therefor --while--; and

line 30, delete "recognised" and insert therefor --recognized--.

Page 19, line 25, delete "recognises" and insert therefor --recognizes--.

Page 20, line 6, delete "send" and insert therefor --sends--;

line 25, delete "at an";

line 26, delete "minimising" and insert therefor --minimizing--;

line 26, after "due" insert -- to--; and

line 26, delete "utilises" and insert therefor --utilizes--.

IN THE CLAIMS

Page 22, line 1, delete "Claims" and insert therefor --What is claimed is:--.

Please cancel claims 1-15 and add new claims 16-30 as follows.

--16. A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network via a Security Gateway, the method comprising the steps of:

(1) negotiating at least one Security Association between the mobile host and a correspondent host of a Virtual Private Network ;

(2) initiating a communication between the mobile host and the Security Gateway and sending an authentication certificate to the Security Gateway, the certificate including data identifying a Security Association which will be used for subsequent communication between the mobile host and the correspondent host; and

(3) sending data packets from the mobile host to the correspondent host using the identified Security Association, via the Security Gateway;

wherein said data packets are forwarded by the Security Gateway to the correspondent host only if they are authenticated by the Security Gateway.

17. The method according to claim 16, comprising the additional steps, prior to step (2), of negotiating at least one Security Association between the mobile host and the Security Gateway and sending said authentication certificate to the Security Gateway using one of the at least one Security Associations between the mobile host and the Security Gateway.

18. The method according to claim 16, wherein said authentication certificate comprises data indicating an IP address of the mobile host.

19. The method according to claim 16, wherein said at least one Security Association is an IPsec phase 2 Security Association and is used on top of an Internet Security Association Key Management Protocol Security Association.

20. The method according to claim 19, wherein said authentication certificate contains Internet Security Association Key Management Protocol cookies of the mobile host and said correspondent host with which the phase 2 negotiation was done.

21. The method according to claim 16, wherein the Security Gateway is coupled between the intranet and a core network of a mobile wireless telecommunications system.

22. The method according to claim 16, wherein the mobile host is a wireless host coupled to the Security Gateway via an access network.

23. The method according to claim 16, wherein the Virtual Private Network comprises an intranet, with the Security Gateway being coupled between the intranet and the Internet.

24. The method according to claim 23, wherein said correspondent host resides within the intranet and said data packets are forwarded to the correspondent host from the Security Gateway over a secure connection.

25. The method according to claim 16, wherein a negotiated Security Association expires after a predefined volume of data has been sent using the Security Association.

26. The method according to claim 16, wherein a negotiated Security Association is time limited by the Security Gateway and, after a predefined time limit, the Security Association is suspended by the Security Gateway.

27. The method according to claim 16, wherein the data packets sent in step (3) and which contain user data are authenticated by the Security Gateway using authentication data sent in separate data packets.

28. The method according to claim 17, wherein the data packets sent in step (3) and which contain user data are authenticated by the Security Gateway using authentication data sent in separate data packets, and wherein the data packets containing user data are sent using a Security Association negotiated between the mobile host and said correspondent host and the data packets containing authentication data are sent using a Security Association negotiated between the mobile host and the Security Gateway.

29. A Security Gateway of a Virtual Private Network, the Security Gateway enabling secure communication between a mobile host and a correspondent host, the Security Gateway comprising:

(1) means for negotiating one or more Security Associations between the mobile host and the Security Gateway ;

(2) means for subsequently initiating a communication between the mobile host and the Security Gateway using a negotiated Security Association and for receiving an authentication certificate sent from the mobile host, the certificate including data identifying the mobile host and an IP address of the mobile host;

(3) means for receiving data packets sent from the mobile host and for authenticating the data packets; and

(4) means for forwarding the data packets from the Security Gateway to said correspondent host only if the received data packets are authenticated.

30. A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network, the method comprising the steps of:

- (1) negotiating one or more Security Associations between the mobile host and a Security Gateway of a Virtual Private Network ;
- (2) initiating a communication between the mobile host and the Security Gateway using a negotiated Security Association and sending an authentication certificate to the Security Gateway, the certificate including data identifying the mobile host and an IP address of the mobile host;
- (3) sending data packets from the mobile host to the Security Gateway and authenticating the data packets at the Security Gateway; and
- (4) forwarding the data packets from the Security Gateway to said correspondent host only if the received data packets are authenticated.--

IN THE ABSTRACT

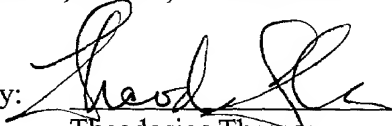
Please delete the Abstract and insert the new Abstract attached as a separate sheet.

REMARKS

The specification has been amended, and the claims and Abstract have been replaced to place the application in better form for examination. Favorable consideration is respectfully solicited.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: 
Theodosios Thomas
Registration No. 45,159

P.O. Box 1404
Alexandria, Virginia 22313-1404
(919) 941-9240

Dated: January 18, 2001

"Express Mail" mailing label No. 2581399173US

Date of Deposit 01/18/01

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

J. Sneed
(Type or printed name of person mailing paper or fee)


(Signature of person mailing paper or fee)

Abstract

A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network. The method comprises negotiating one or more Security Associations between the mobile host and a correspondent host of a Virtual Private Network . Subsequently, a communication is initiated between the mobile host and a Security Gateway and an authentication certificate sent to the Security Gateway, the certificate containing at least the identity of a Security Association which will be used for subsequent communication between the mobile host and the correspondent host. Data packets can then be sent from the mobile host to the correspondent host using the identified Security Association, via the Security Gateway. However, the data packets are forwarded by the Security Gateway to the correspondent host only if they are authenticated by the Security Gateway.